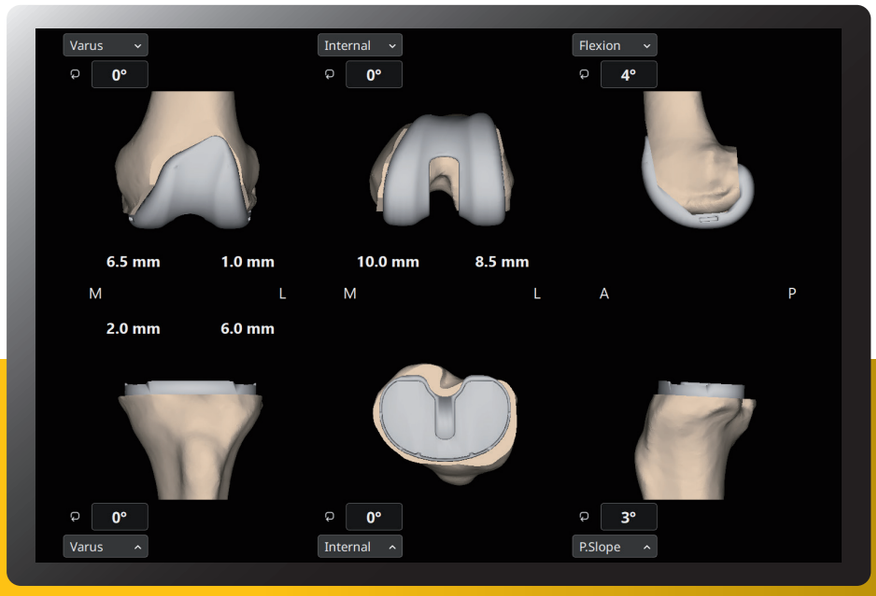
# Ortho Slice™ 3D Knee Planning

## Security Operations Manual

REF: 6007-670-000




# Table of Contents

# Table of Contents

# 01 Purpose

This Security Operations Manual (SOM) provides information that Stryker's customers need to know in order to integrate a specific Stryker device or health IT solution into a customer's IT network environment in a secured manner.

It also supports customer's ability to perform risk management, to identify configurable security controls, and to better protect their systems.

# 02 Definitions

## API – Application Programming Interface

An interface for computing that defines interactions between multiple software intermediaries.

## COTS – Commercial off-the-shelf

Software (or any other item) that is sold as a packaged solution which is then adapted to satisfy the needs of the organization purchasing the COTS. Some medical devices utilize COTS software in addition to or instead of software developed by the manufacturer.

Refer- third-party software.

## Customer

The individual or organization responsible for procurement and operation of the device. See Owner and Operator.

## Device

The item being integrated or used for a healthcare purpose. A Medical Device or other health IT product may be referred to as a Device or a Product in this document.

## DICOM (Digital Imaging and Communications in Medicine)

Standard developed by NEMA and the American College of Radiology, used worldwide to store, exchange, and transmit medical images.

## FDA – U.S. Food and Drug Administration

A federal agency of the United States' Department of Health and Human Services.

Refer www.fda.gov

## HDO – Healthcare Delivery Organization

Also "Health Delivery Organization," an organization or group of organizations that are involved with the delivery of healthcare services. A hospital is an HDO. If an HDO purchases and operates a Stryker device, the HDO is also the Customer, Owner, and Operator per the definitions of those terms.

## IEC – International Electrotechnical Commission

A global organization whose work underpins quality infrastructure and international trade in electronic goods. IEC publishes thousands of international standards, including documents related to medical device software (for example, IEC 62304).

Refer www.iec.ch.

## IFU – Instructions for Use

Information provided by the manufacturer in document or electronic form, informing the user of a device's intended purpose and proper use and of any precautions to be take.

## ISO – International Organization for Standardization

An international standard-setting body that promotes proprietary, industrial, and commercial standards, and publishes standards relevant for information technology, privacy, and security (for example, ISO/IEC 27034).

Refer www.iso.org

## Manufacturer

The entity (Stryker) that builds the device and sells it to the customer.

## MDR – European Union (EU) Medical Device Regulation of 2017

The European Union regulation concerning medical devices.

Refer https://ec.europa.eu/health/md_sector/overview_en

## Medical Device

See the following sources if a precise definition is required: FDA, MDR (EU) 2017/745, ISO 14971:2007.

## NEMA – National Electrical Manufacturers Association

Refer www.nema.org

## NIST - National Institute of Standards and Technology

A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. NIST has published comprehensive standards for the selection, implementation, and risk management of security and privacy controls (e.g., NIST SP 800-53).

Refer www.nist.gov.

## Operator

The person(s) using the device for its intended purpose. This term may also sometimes refer to the person or organization responsible for procuring the device (owner, customer).

## OSS – Open-Source Software

Third party software licensed under an OSS license, in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose as long as the license terms are adhered to.

## Owner

See Operator and Customer.

## PHI - Protected Health Information

Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media; or transmitted, or maintained, in any other form or medium (source: extracted from 45 CFR Section 160). Note: This is a subset of PII.

## PII - Personally Identifiable Information

Any information about an individual maintained by an agency, including the following:

- Any information that can be used to distinguish or trace an individual's identity.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (source: from NIST SP 800-122).

## Product

See Device.

## SaMD - Software as a Medical Device

Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (source: from International Medical Device Regulators Forum).

## SBoM – Software Bill of Materials

For a specific device, a listing of all software components that are incorporated into the final product. The SBOM may be used to assist with operational security planning by the HDO.

## SOM - Security Operations Manual

A product-specific guide to the secure integration of a product into a customer IT network (this document).

## Third-party software

Third party software is software not developed by Stryker, and for which Stryker otherwise does not have complete ownership. See COTS and OSS.

## User

See Operator.

# 03 Product Description

This Security Operations Manual (SOM) provides information that Stryker's customers need to know in order to integrate a specific Stryker device or health IT solution into a customer's IT network environment in a secured manner.

It also supports customer's ability to perform risk management, to identify configurable security controls, and to better protect their systems.

| | |
|---|---|
| **Manufacturer Name** | stryker |
| **Stryker Division** | Stryker Global Technology Center |
| **Address** | **Stryker Global Technology Center Private Limited**<br><br>10th Floor, Vatika Business Park,<br>Block Two, Sector-49 ,Sohna Road,<br>Gurgaon 122002, Haryana, India |
| **Device Description** | Ortho Slice 3D Knee Planning software is used to create a pre-operative planning for a knee replacement surgery where Stryker's Triathlon knee implant is used.<br>The Ortho Slice 3D Knee Planning software is intended to provide a surgeon facing, easy to use knee planning software, that uses the patient's CT scans to visualize the disease condition of Knee in three-dimension and enable effective decision making for the surgeons before they even go into the operating room on the day of the surgery. |
| **Device Model, Version** | **6007-670-000 V1.0 (Further digits for minor fixes controlled internally)** |
| **Manufacturer Contact Information** | **Manufacturer:**<br><br>**Stryker Global Technology Center Private Limited**<br>10th Floor, Vatika Business Park, Block Two, Sector-49,<br>Sohna Road, Gurgaon 122002, Haryana, India<br><br>**Distributed By**:<br><br>**Stryker Japan K.K**.<br>2-6-1, Koraku, Bunkyo-ku,Tokyo, 112-004, Japan<br>t/f: 03-6894-0000<br><br>Additional information and contact links are available on Stryker's Product Security webpage, https://www.stryker.com/us/en/about/governance/cyber-security.html. |

*Table 1.1 Product Description*

## 3.1 Device and Manufacturer Identification

### Device:

Ortho Slice 3D Knee Planning Software

## Manufacturer:

**Stryker Global Technology Center Private Limited**

10th Floor, Vatika Business Park
Block Two, Sector-49, Sohna Road,
Gurgaon 122002, Haryana, India

# 3.2 Device Intended Use:

The Ortho Slice 3D Knee Planning software is intended to provide a surgeon facing, easy to use knee planning software, that uses the patient's CT scans to visualize the disease condition of the knee in three dimension and enable effective decision making for the surgeons before they even go into the operating room on the day of the surgery.

**Functionality Includes:**

- Auto-segmentation and landmark identification (manual modification possible)
- Effortless implant planning
- Saves the planned report for quick reference, the surgeon has the control and can choose how to interpret and use the results from the pre-operative planning.

**Contraindication**:

The surgeon needs to determine whether the patient's conditions are appropriate for this kind of procedure. The patients who have other type of metallic implants at or near Knee, Ankle, or Hip joints, which can create artifacts/noise on the CT Scan, are against the use of this system. In addition, some patients with advanced osteoporosis or deformities would be contraindicated like fused bone in the femur and tibia at the knee region. Reads only CT data.

Refer IFU and User Manual for more details.

# 3.3 Vulnerability Intake and Monitoring:

When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability's exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the customer in a timely manner. Vulnerability information may also be requested from Stryker at any time.

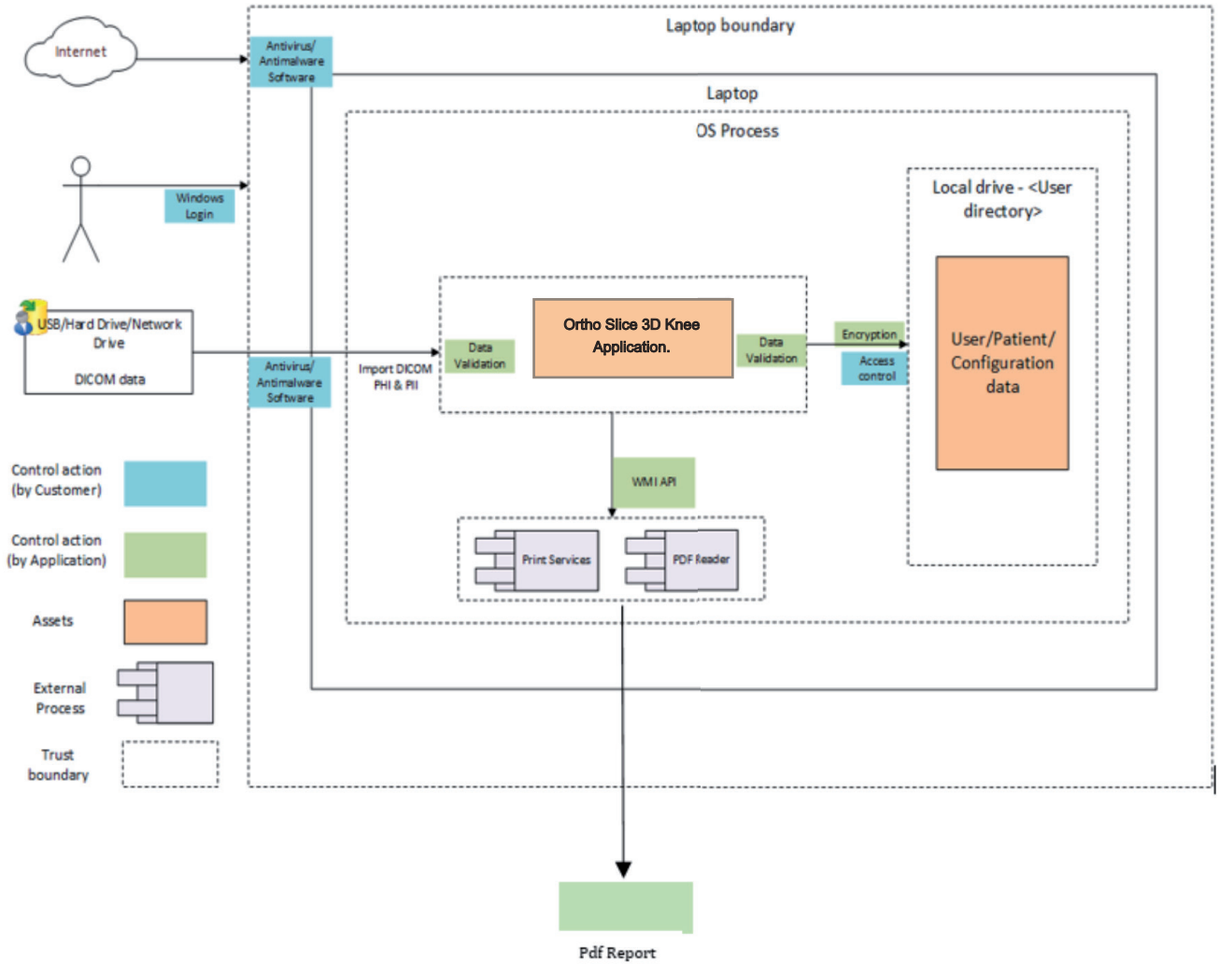
Any potential security vulnerabilities customer may become aware of due to Ortho Slice 3D Knee Planning software must be communicated to Stryker customer care and the same will be handled through the post market complaints management process to do the assessment and required actions including any updates needed for the customers.

# 3.4 System Characterization and System Assets

Ortho Slice 3D Knee Planning software allow surgeon to create preoperative planning before proceeding to the surgery (Conventional or Navigated). This application allows to import/load Patients DICOM CT images from external storage devices such as USB, Hard disk and network drive. This application will not allow user to transfer the patient data to any other external or connected system to process further. All the patient data is encrypted and stored locally under the logged user folder.

## 3.5 System Security Context and Intended Environment

*Figure 1: System Security*




While there is no specific requirement for Ortho Slice 3D Knee Planning software to be fully functional other than a usual windows environment, however Stryker recommends the user to follow some of the best practice security standards in order to run the application in a safe and secure environment as follows:
Devices operating in the intended use environment should consider that their IT infrastructure must follow different risk management approaches associated with their networks. HDO or customer must adopt a risk management process adhering to general cybersecurity best practices to maintain the healthcare provider's overall security status and their secure environment, as follows:

- Good physical security to prevent unauthorized physical access to Ortho Slice 3D Knee Planning software application.
- Access control measures (for example, role based) to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services and applications.
- General patch management practices that ensure timely security patch updates.
- Malware protection to prevent unauthorized code execution.
- Security awareness training.

## 3.6 Setup of the SaMD (Software as a Medical Device) Ortho Slice 3D Knee Planning

The Ortho Slice 3D Knee Planning software operates on Window-based PC

| Specifications | Description |
|---|---|
| **Operating System** | Windows 10 version |
| **CPU** | Intel Core i7-4770 or higher |
| **RAM** | 32 GB or more |
| **Disk space** | 12 GB for program installation, 500GB or more for patient data storage |
| **Monitor resolution** | 1920*1080 pixels or above |
| **Graphics** | Dedicated 4GB or higher memory (for example, Nvidia Quadro RTX3000 or NVIDIAT600) |
| **Communication port** | USB 2.0 or higher |
| **Optional mouse with left and right button, and scroll** | |

**Note:**

- For cases where the patient data is loaded from local network drive, ensure network connectivity before starting the system. If there is a disruption in network connectivity, loading the data may take longer time than usual. If there is a disruption in network while loading the case, the software will notify the user.
- Information for compatibility with other devices. External hard drive to transfer CT data should be compatible with USB 2.0 or higher.
- For other Security related requirements please refer this manual

# 04 Management of PII and PHI

Ortho Slice 3D Knee Planning software does not process PII /PHI outside the surgeon's laptop. The HDO has full control of it is laptop including the Ortho Slice 3D Knee Planning software and responsibility for any PII /PHI there. The software will only display the PII /PHI information from the DICOM CT data or entered by the Surgeon and will not process it outside of the surgeon's laptop boundary. The HDO and User has the full control of the PHI and PII data in the Laptop and if any data to be removed based on the HDO data retention Policies, the HDO/ User can take support from Stryker to remove the data not needed to be retained.

## 4.1 Handling of Patient Requests for their PHI Access

“Refer to Section Management of PII and PHI” above. User/ HDO has full control on patient data kept on laptop. Application do not have any additional functionality to provide access for patient requests. The HDO need to take the Report Output and share with Patients in cases where the Patient request his Personal Health Information as per the HDO process

## 4.2 Storage and Removal of PII

Stryker does not process outside the surgeon’s laptop. The HDO has full control of it is laptop including the Ortho Slice 3D Knee Planning software and responsibility for any PII there.

PII is embedded in the input DICOM files provided by the surgeon to the software. The software uses the PII data to display on its GUI and final planning PDF contains the PII information from DICOM files.

PII data will be maintained in volatile memory within the user laptop and can be exported to a PDF file. PII data is not transferred to any other system. User has the provision to anonymize the Patient Name on the Software GUI for the purpose of presenting the data for any external stake holders for training or other needs to support any privacy requirements for the HDO.

For backup and restore of PII data, please reach out to Stryker customer care for support if needed.

# 05 Automatic Log-Off

Customers are advised to configure windows OS to automatically lock the screen after a period of idle time as per the HDO IT policies.

Application also has the ability to lock the screen after inactivity for configurable timeout. User can configure the inactivity timeout. For details, please refer User Manual Section To configure System Settings.

# 06 Audit Controls

Stryker uses strong protection mechanism to protect the audit logs from getting tampered by any unauthorized party and hence does not require any extra steps from the users. Audit logs are encrypted using 256-bit AES encryption to avoid any tampering of the information. Decryption of the audit log is handled by Stryker on request from authorities. User cannot edit or alter the audit logs.
Ortho Slice 3D Knee Planning Software captures the following type of audit events:

- Creation/modification evets of patient PII data (No PII data stored)
- Import of DICOM data from removable media
- Application Programming Interface (API) and similar activity – Used for Printing and PDF view.
- Marked data with time stamp information to enable it to be selected for deletion based on when it was acquired or stored. Work step visited, save / update operation on patient data. Application data - workflow and features executed.

Audit Logs Format is: <timestamp>,<user>,<component>,<Feature/Module>,<Action>

It is possible to export the logs via physical media considering the physical media like USB etc. to be secure. But it is recommended for the users to keep their physical media secure and updated against the latest threats.

Below are some of the safety measures that can be implemented to secure physical media like USB drive.

### Do not plug a USB drive into an unknown computer

Do not plug the USB into any computer without verifying the identity and safety of that computer system as the system may pose a potential security threat to your physical device.

### Take advantage of security features

Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.

### Disable Autorun

The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. Disabling Autorun prevents malicious code on an infected USB drive from opening automatically.

### Use and maintain security software and keep all software up to date

Use a firewall, antivirus software, and anti-spyware software to make your computer less vulnerable to attacks and keep the virus definitions current. Also, keep the software on your computer up to date by applying any necessary patches.

## 07 Authorization

Ortho Slice 3D Knee Planning software requires a valid license in order to be fully functional and running., which needs to be obtained from Stryker only. Apart from requiring a valid license, the application user must leverage windows authentication and authorization mechanism for user access to software and data. So, Stryker best recommends the user to setup proper authorization of users on their laptops as discussed below.

Authorization in system security is the process of giving the user permission to access a specific resource or function. In secure environments, authorization must always follow authentication. Users should first prove that their identities are genuine before an organization’s administrators grant them access to the requested resources. So proper authorization must be implemented at system level to harden the security. Different approaches to authorization may include

### Role-Based Access Control (RBAC)

Users are identified as being in a role that stipulates what privileges they have. Additionally, their user ID would restrict what data they have access to.

### Access Control Lists (ACL)

An ACL specifies which users have access to particular resources. For instance, if a user wants to access a specific file or folder, their username or details should be mentioned in the ACL in order to be able to access certain data.

## 7.1 Access Prevention

Ortho Slice 3D Knee Planning software does not have any built-in access prevention features enabled in the Ortho Slice 3D Knee Planning software and leverages windows access prevention mechanism. It is recommended to customers to have proper access control measures as discussed in the below sections.

Taking steps to prevent unauthorized access to the system and its software components is important for a wide number of reasons, including preventing others from installing spyware and deleting your important files, or even creating viruses. By making changes to your computer to prevent unauthorized access, you are also protecting your personal privacy. Here are some steps to take to properly secure your computer and prevent others from accessing or modifying your application data:

- Set up password protection for user authentication: Password protection must be enabled at system level so that any unauthorized user cannot access the system. Password should be set in such a way that it must not be easy to guess. Also, strong password policy must be implemented to enhance the overall security of the system
- Install antivirus software or a spyware protection program: A good antivirus or spyware protection program must be installed on the system. These programs are used to detect any malicious actions or programs that might be used as a threat for the system or installed application. Lastly these antivirus programs must be regularly updated so that it can protect the system and the installed applications from latest security threats.
- Restrict the access to your system only to a limited number of trusted peoples. This can help the installed application to be accessed only by an authorized individual.

## 7.2 Privilege and Access

Stryker recommends the laptop administrator to create separate users with appropriate privileges for access to Ortho Slice 3D Knee Planning software on the same laptop. Privilege and access to the Ortho Slice 3D Knee Planning software must be restricted such that any user of the application can only use it within its intended use and any other functionality outside of the scope of the application is restricted as much as it can be. Users can maintain their own data on same laptop without access to other user's data by setting different log in access.

# 08 Cyber Security Product Upgrades

The application does not have any updates installation policy implemented. Hence the users will not get any online updates. If any potential vulnerabilities are identified by Stryker which require an update at the customer site, a new version of the software will be released, and customers will be informed about the action to be taken at their end.

It is HDO's responsibility to update the latest patches for their operating system, their third-party components (if any) and other applications like Virus Protection software's/anti-malware software's, firewalls etc. Timely to ensure the security and protection of the system.

Ortho Slice 3D Knee Planning software does not contain any malware protection embedded in it. Hence, users are advice to install and anti-malware software on laptop.

# 09 Health Data De-Identification

Ortho Slice 3D Knee Planning software anonymizes the data at runtime but does not delete or remove them. This can be done via GUI interface of the application itself.

Refer User Manual Section Additional tools for more details.

# 10 Data Backup and Disaster Recovery

The application does not contain any online or offline mode of data backup or its recovery. So, the users are expected to have their own copy of data backup possibly in any physical media or via some online storage methods.

# 11 Health Data Integrity and Authenticity

No user actions are needed since any health data or other sensitive data stored on the system is encrypted using strong 256-bit AES encryption algorithm by the application itself to preserve the data integrity. The application properly checks the integrity of the data before loading them.

# 12 Malware Detection/Protection

The standalone Ortho Slice 3D Knee Planning software by default does not contains any malware detection functionality and requires the user to have some malware detection in place. As, the malware detection is crucial with malware's prevalence because it functions as an early warning system for the computer secure regarding malware and cyberattacks. It keeps hackers out of the computer and prevents the information from getting compromised. This involves the process of scanning the computer and files to detect malware.

To protect against the malwares below points are recommended:

- Install a good malware detection program on the system
- Keep your computer and software updated
- Use a non-administrator account whenever possible
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Do not trust pop-up windows that ask you to download software
- Limit your file sharing

## 12.1 Other Compensation/Protection Controls

The Ortho Slice 3D Knee Planning Software application contains several protection mechanisms by its design like the application requires a valid license in order to work properly, the logs are encrypted using private keys and the data de-identification is also done which anonymizes the data at runtime. Besides these projections in place, Stryker recommend the users to apply certain other safety measure as below:

- The application should be allowed to be run only as authorized individual enabled using built in mechanism of windows OS.
- Proper Application whitelisting should be done on all security agents running on the device so that the

Ortho Slice 3D Knee Planning software is not flagged as malicious in any case.

- Any third-party components installed in the system must be properly updated.
- Regular Antivirus scan should be done in order to eliminate any possible threats.
- Application Logs shall be audited for any errors or proper functioning of the application.
- Regular windows updates and patches should be installed.

## 12.2 Firewall Implementation

In order to safely use the application its important the below listed firewall rules be strictly followed and respected while using the application:

Ensure that you have enabled the firewall. If not, please follow the below steps on your Windows computer

1. From the Start menu, click Control Panel
2. Select System and Security. Click Windows Defender Firewall
3. Click Turn Windows Firewall on or off
4. Select Turn on Windows Firewall for domain home/work (private) or public network

### Other things to consider:

- It is imperative that logs/warnings get the attention of the user. Any anomaly must then be resolved after its addressed.
- Ensure that ports necessary for function are accessible only to authorized clients of the application.
- In case a malware was reported on the system, ensure a proper sweep scan has been initiated and the removal of the malware was successful before resuming normal operations.

Firewall helps in preventing network access to devices. If properly used and configured it can lead to protected and reliable accessibility. It can help in prevention of unauthorized access and network connections against external threats, IP spoofing & routing attacks and malicious packets.

# 13 Connectivity Capabilities

The Ortho Slice 3D Knee Planning software application by default does not require any network connectivity or even wireless connectivity for its operation. The input CT data can be loaded from a network drive and the HDO IT to ensure adequate security controls to protect the network drive connected to the Laptop where Ortho Slice 3D Knee Planning software is installed. Also, it does not apply any restrictions in place when the physical media needs to be inserted in the system for data backup or data transmission.

So, it is advised for the users to use only secure and updated physical media in case it is required. To secure the USB or any physical media its best to properly scan them using a good antivirus program.

# 14 Personal Authentication

Ortho Slice 3D Knee Planning software does not provide any authentication mechanism apart from requiring a valid license which is unique for the system in order to be operational.

Stryker recommend the user to implement the secure windows authentication using strong password-based authentication on their laptop. These passwords should be strong enough which is not easy to guess. Also, it must contain alphanumeric characters along with special characters to ensure best security practice.

For proper user management, the system should be configured for the below points.

- The authentication system should be done via password-based login or integrated windows-based authentication
- After a few unsuccessful attempts account must lockout
- Passwords must be changed after a regular interval of time
- Default password or easy guess password must not be accepted by the system. In other words, the password should meet the password complexity policy
- The system must be configured in such a way as to lock if it is left idle after a reasonable period
- Physical security must also be implemented to manage access to the system

# 15 Roadmap for Third Party Components in Device Life Cycle

Stryker has evaluated third -party components as per the requirement identified in IEC 62304 and adequate actions are implemented in application.

Stryker will be evaluating high-risk third-party components periodically and communicate to customers for any updates required during the product lifecycle.

# 16 System and Application Hardening

Stryker had performed the application security testing and security code review of Ortho Slice 3D Knee Planning software. Ortho Slice 3D Knee Planning software is hardened by eliminating any vulnerability or flaw, which can lead to security issue.

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in the application, systems, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, so on. attackers and malware have fewer opportunities to gain a foothold within the IT ecosystem. Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities. The type of hardening carried out depends on the risks in the existing technology, the resources that are available, and the priority for making fixes.

Stryker recommends to customers to keep below key points while implementing the system hardening.

## Audit your existing systems

Carry out a comprehensive audit of the existing technology. Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the system where the application is installed and prioritize fixes

## Create a strategy for systems hardening

There is no need to harden all the systems at once. Instead create a strategy and plan based on risks identified within the technology ecosystem and use a phased approach to remediate the biggest flaws.

## Patch vulnerabilities immediately

Ensure to have an automated and comprehensive vulnerability identification and patching system in place.

### Network hardening

Ensure the firewall is properly configured and that all rules are regularly audited; secure remote access points and users; block any unused or unneeded open network ports; disable and remove unnecessary protocols and services; implement access lists; encrypt network traffic.

Also refer to Section 13

### Operating system hardening

Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.

### Eliminate unnecessary accounts and privileges

Enforce least privilege by removing unnecessary accounts (such as orphaned accounts and unused accounts) and privileges throughout the IT infrastructure.

### Anti-Malware installation

The system running Ortho Slice 3D Knee Planning software should have proper anti-malware software installed with latest updates.

## 17 Health Data Storage Confidentiality

The data at rest is encrypted using a strong encryption mechanism implemented within the application which safeguards the sensitive medical data from prying eyes.

## 18 Transmission Confidentiality

Ortho Slice 3D Knee Planning software does not transmit the data over network or internet. End user inputs data into the software using removable media or from local system. The pdf output can be stored or exported on the removable media.

Below are some of the guidelines to the user to be followed while managing data confidentiality:

### Manage data access

Controlling confidentiality is, in large part, about controlling who has access to data. Ensuring that access is only authorized and granted to those who have a “need to know” goes a long way in limiting unnecessary exposure. Users must also authenticate their access with strong passwords and, where practical, two-factor authentication. Periodically review access lists and promptly revoke access when it is no longer necessary.

### Physically secure devices

Controlling access to data includes controlling access of all kinds, both digital and physical. Protect devices from misuse or theft by storing them in locked areas. Never leave devices or sensitive documents unattended in public locations.

### Securely dispose of data

When data is no longer necessary for any-related purposes, it must be disposed of appropriately.

### Manage data acquisition

When collecting sensitive data, be conscious of how much data is actually needed and carefully consider privacy and confidentiality in the acquisition process. Avoid acquiring sensitive data unless necessary; one of the best ways to reduce confidentiality risk is to reduce the amount of sensitive data being collected in the first place.

### Manage data utilization

Confidentiality risk can be further reduced by using sensitive data only as approved and as necessary. Misusing sensitive data violates the privacy and confidentiality of that data and of the individuals or groups the data represents.

### Manage laptop

Computer management is a broad topic that includes many essential security practices. By protecting devices, you can also protect the data they contain. Follow basic cybersecurity hygiene by using anti-virus software, routinely patching software, whitelisting applications, using device passcodes, suspending inactive sessions, enabling firewalls, and using whole disk encryption.

# 19 Security Program Integration

Ortho Slice 3D Knee Planning software is a standalone software installed on user laptop. The secure practices for the software are covered under Section 8 of this document.

Stryker has implemented incident response programs as part of complaint handling process for the product. The product is intended for Japan market only and user can call t/f: 03-6894-0000 to inform Stryker if any potential threat is identified in the software. Then, Stryker team will take the right steps to help the customer to deal with the situation. Stryker has done extensive security testing of the Ortho Slice 3D Knee Planning software application and implemented adequate actions to ensure protection from external threats. However, beyond this security measures in place, it is advised for the users to take a step ahead and follow some of the below guidelines to ensure better security postures.

- Do not plug any unknown physical media like USB etc. If it is required to plug in to the device, it must be scanned thoroughly using a strong anti-malware program.
- System must be scanned on a regular basis for any potential threats using Anti-malware and/or anti-virus softwares

## 19.1 Risk Management

Stryker integrates cyber security risk management into its overall program for health and safety risk management. Both security and safety risk assessments were conducted for this device per guidelines in compliance with EN/ISO 14971 and Stryker Product Security procedures. Additionally, Stryker has a robust post-market security risk management process that monitors the ongoing security posture of this device and addresses any security incidents that might arise.

# 20 Secure Decommissioning

Please reach out to Stryker Customer Care for secured decommissioning.

# Japanese

日本

# Table of Contents

# Table of Contents

# 01 目的

このセキュリティ運用マニュアル（SOM）は、特定のStrykerデバイスまたは医療ITソリューションをカスタマーのITネットワーク環境に安全な方法で統合するために、Strykerのカスタマーが知っておく必要がある情報を提供するものである。

また、これはカスタマーがリスク管理を行い、設定可能なセキュリティコントロールを特定し、システムをより良く保護することをサポートする。

# 02 定義

## API–アプリケーション・プログラミング・インターフェース

これは複数のソフトウェア中継の相互作用を定義した、コンピューターの利用のためのインターフェースである。

## COTS–商用オフザシェルフ

ソフトウェア（またはその他のアイテム）は、パッケージソリューションとして販売され、その後、COTSを購入する組織のニーズを満たすように適合されます。医療デバイスの中には、製造者が開発したソフトウェアに加えて、またはその代わりに、COTSソフトウェアを利用するものがある。

参考:第三者のソフトウェア.

## カスタマー

デバイスの調達および運用に責任を持つ個人または組織である。所有者、運営者を参照。

## デバイス

医療目的のために統合される、または使用される品目である。本書では、医療デバイスまたはその他の医療IT製品を、デバイスまたは製品と呼ぶことがある。

## DICOM (医療におけるデジタル画像と通信)

NEMAと米国放射線学会によって氷刃的に開発されて、医用画像の保存、交換、伝送に世界中で使用されている規格である。

## FDA–米国食品医薬品局

米国保健社会福祉省の連邦機関である。.

www.fda.govを参照してください。

## HDO–医療提供組織

「Health Delivery Organization」は、医療サービスの提供に関わる組織またはそのグループである。病院はHDOに該当する。HDO が Stryker のデバイスを購入し、運用する場合、HDO は、これらの用語の定義に従って、カスタマー、所有者、およびオペレーターでもある。

## IEC–国際電気標準会議

品質インフラと電子製品の国際貿易を支える世界的な組織である。IECは、医療デバイスソフトウェアに関する文書（IEC 62304など）を含む数千の国際規格を発行している。

参考:www.iec.ch.

## IFU–製品の使用説明書

デバイスの意図する用途や適切な使用方法、および注意事項をユーザーに通知するための製造者が文書または電子形式で提供する情報である。

## ISO –国際標準化機構

情報技術、プライバシー、セキュリティ（例:ISO/IEC 27034など）に関連する規格を発行している 独自規格、工業規格、商業規格を推進する国際標準化団体である。 参考:www.iso.org

## 製造業者

デバイスを製造し、カスタマーに販売する事業体（Stryker）である。

## MDR–年度欧州医療デバイス規則

医療デバイスに関する欧州連合（EU）の規制である。.

参照: https://ec.europa.eu/health/md_sector/overview_en

## 医療デバイス

正確な定義が必要な場合は、以下の出典:FDA, MDR (EU) 2017/745, ISO 14971:2007を参照してください。

## NEMA–全米電気デバイス製造業者協会

参考:www.nema.org

## NIST-米国標準技術研究所

物理科学の研究所であり、米国商務省の非規制機関である。NISTは、セキュリティおよびプライバシー管理の選択、実装、およびリスク管理のための包括的な規格を発行している。（例:NIST SP 800-53など）。

参考:www.nist.gov.

## オペレーター

意図された目的のためにデバイスを使用する人である。この用語は、デバイスの調達に責任を持つ個人または組織（所有者、カスタマー）を指すこともある。

## OSS –オープンソースソフトウェア

OSSライセンスとは、著作権者がライセンス条項を遵守する限り誰にでもどのような目的でも、ソフトウェアを使用、研究、変更、配布する権利をユーザーに許諾するものである。

## 所有者

オペレーターとカスタマーを参照してください。

## PHI-保護対象保健情報

電子媒体で伝送される、電子媒体で維持される、またはその他の形態や媒体（出典:45 CFR Section 160より抜粋）で伝送、維持される個人を特定できるヘルス情報（IIHI）である。注:これはPIIのサブセットである。

## PII - 個人を特定できる情報

機関が保持する個人に関するあらゆる情報であって、以下を含む。

- 個人の身元を識別または追跡するために使用できるすべての情報。

· 医療、教育、財務、雇用に関する情報など、個人とリンクしているか、リンク可能なその他の情報（出典:NIST SP 800-122より）。

## 製品

デバイスを見る.

## SaMD-医療デバイスとしてのソフトウェア

1つ以上の医療目的のために使用されることが意図され、ハードウェア医療デバイスの一部とならずにこれらの目的を実行するソフトウェア（出典:国際医療デバイス規制機関フォーラムより）である。

## SBoM–ソフトウェア部品表

特定のデバイスについて、最終製品に組み込まれるすべてのソフトウェアのコンポーネントのリストである。SBOMはHDOによる運用上のセキュリティ計画を支援するために使用されることがある。

## SOM -セキュリティ運用マニュアル

カスタマーのITネットワークに製品を安全に組み込むための製品別案内書（本書）である。

## サードパーティ製ソフトウェア

第三者製ソフトウェアとは、ストライカーが開発したものではなく、ストライカーが完全な所有権を有していないソフトウェアを指す。COTS および OSS を参照してください。

## ユーザー

オペレーターを見る

# 03 製品説明

このセキュリティオペレーションマニュアル（SOM）は、Stryker のカスタマーが、特定の Stryker デバイスまたは医療 IT ソリューションを、カスタマーの IT ネットワーク環境に安全な方法で組み込む場合に統合するために知っておく必要がある情報を提供するものである。

また、カスタマーがリスク管理を行い、設定可能なセキュリティコントロールを特定し、システムをより良く保護することをサポートする。

| | |
|---|---|
| **製造者名** | stryker |
| **ストライカー事業部** | ストライカー･グローバル･テクノロジー･センター |
| **住所** | **ストライカー・グローバル・テクノロジー・センター有限会社**<br><br>ヴァティカ･ビジネス･パーク, 第2ブロック10階, セクター-49, ソーナロード･グルガオン 122002 ハリヤナ州, インド |
| **デバイスの説明** | オーソオーソスライス3Dニープランニングソフトウェアは、Stryker社のインプラントであるトライアスロンを使用した人工膝関節置換術の術前プランニングを作成するために使用されている。<br><br>オーソスライス3Dニープランニングソフトウェアは、患者のCT画像を用いて病態を3次元で可視化し、手術当日に手術室に入る前に意思決定ができるような、外科医向けの使いやすいプランニングソフトウェアを提供することを目的とする。オーソスライス3Dニープランニングソフトウェアは、CT画像から作成した3Dデジタルモデルから、膝関節の関節面（大腿骨顆部と脛骨プラトー）を人工関節に置換する計画を立てるためのソフトウェアである。 |
| **機種、バージョン** | 6007-670-000 V1.0 （内部で管理しているマイナーフィックスの桁上げ |
| **メーカー連絡先** | **製造業者:**<br>ストライカー･グローバル･テクノロジー･センター有限会社<br><br>ヴァティカ･ビジネス･パーク, 第2ブロック10階, セクター-49, ソーナロード･グルガオン 122002 ハリヤナ州, インド<br><br>**販売元:**<br>日本ストライカー株式会社<br><br>2-6-1,Koraku,Bunkyo-ku,Tokyo,112-004,Japan<br><br>t/f:03-6894-0000<br><br>その他の情報および連絡先については、Stryker の製品セキュリティウェブページ、https://www.stryker.com/us/en/about/governance/cyber-se- curity.html をご覧ください。 |

表1.1 製品概要

## 3.1 デバイスおよび製造者の識別

**デバイス:**

オーソ スライス 3Dニーナビゲーションソフトウェア

**製造者:**

**ストライカー・グローバル・テクノロジー・センター有限会社**

ヴァティカ・ビジネス・パーク, 第2ブロック10階, セクター-49, ソーナロード・グルガオン 122002

ハリヤナ州, インド

## 3.2 デバイスの使用目的:

オーソスライス3Dニープランニングソフトウェアは、患者のCT画像を用いて病態を3次元で可視化し、手術当日に手術室に入る前に意思決定ができるような、外科医向けの使いやすいプランニングソフトウェアを提供することを目的とする。オーソスライス3Dニープランニングソフトウェアは、CT画像から作成した3Dデジタルモデルから、膝関節の関節面（大腿骨顆部と脛骨プラトー）を人工関節に置換する計画を立てるためのソフトウェアである。

**機能としては以下のものがある。**

- オートセグメンテーションとランドマーク識別（手動修正可能）
- 容易なインプラントプランニング
- 予定されているレポートを保存し、すぐに参照できるようにすることで、術前計画の結果の解釈と利用に関しては術者がコントロールし、選択することができる。

**禁忌事項**

外科医は、患者の状態がこの処置に適しているかどうかを判断する必要があります。CTスキャンにアーチファクトやノイズを発生させる可能性がある膝関節、足関節、股関節に金属製のインプラントがある患者さんは、このシステムの使用には適していません。また、高度な骨粗鬆症や変形を有する一部の患者さんは、膝の大腿骨や脛骨の癒合骨のように、このシステムの使用を禁忌とされています。CTデータは読み取りのみです。

詳細については、IFUおよびユーザーマニュアルを参照してください。

## 3.3 脆弱性の取り込みと監視:

Strykerが監視やその他のソースから脆弱性情報を入手した場合、その脆弱性の悪用可能性と影響の評価が行われる。この評価に基づいてStrykerは、セキュリティ更新の提供やカスタマーへのタイムリーな連絡など、さらなる対応が必要であるかどうかを判断する。また、脆弱性情報はStrykerに要求することができる。

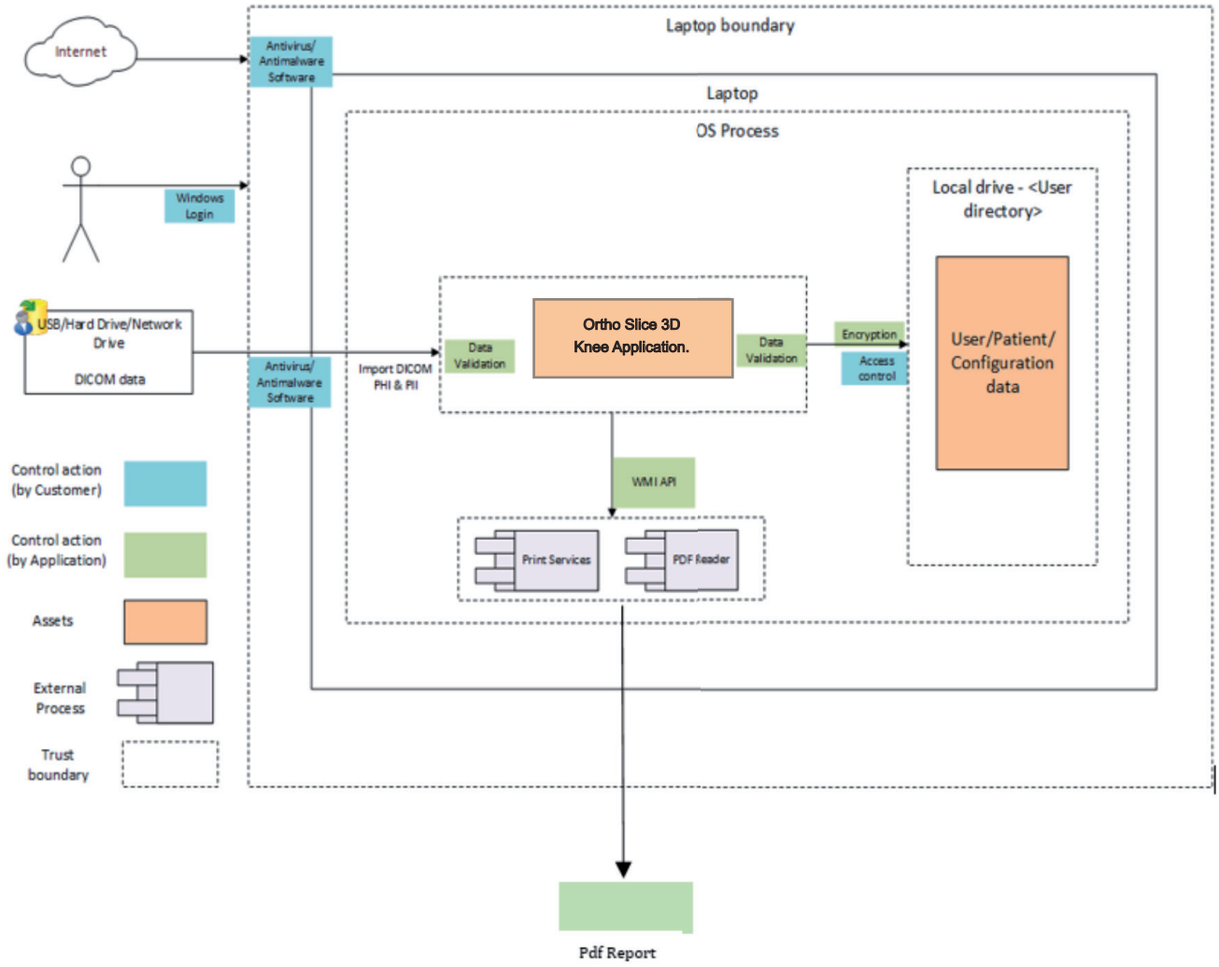
オーソ スライス 3D膝関節プランニングソフトウエアに起因する潜在的なセキュリティ脆弱性について、カスタマーが認識されている場合は、Stryker カスタマーケアにお知らせください。この場合、市販後の苦情管理プロセスを通じて、カスタマーに必要な更新を含む評価と必要な措置を行う。

## 3.4 システムの特性評価とシステム資産

オーソスライス3Dニープランニングソフトウエアは、手術を行う前に、術前計画を作成することができる。このアプリはUSB、ハードディスク、ネットワークドライブなどの外部記憶デバイスから、患者のDICOM CT画像を入力/ロードすることができる。このアプリケーションは、ユーザーが患者データを他の外部システムや接続されたシステムに転送して、更なる処理を許可しない。患者データはすべて暗号化され、ログアウトしたユーザーフォルダーの下にローカルに保存される。

## 3.5 システムセキュリティコンテキストと使用目的環境

図1 システムの安全性




オーソスライス3Dニープランニングソフトウェアが完全に機能するためには、通常のWindows環境以外では特に必要ないが、Strykerは安全でセキュアな環境でアプリを実行するために、以下のような成功事例の安全標準に従うことを推奨している。

意図された使用環境で動作するデバイスは、その IT インフラがネットワークに関連するさまざまなリスク管理アプローチに従わなければならないことを考慮する必要がある。HDOまたはカスタマーは、医療機関の全体的なセキュリティ状況とその安全な環境を維持するために、以下のように一般的なサイバー・セキュリティの成功事例に従ったリスク管理プロセスを採用しなければならない。

- オーソスライス3Dニープランニングソフトウェアのアプリへの不正な物理的アクセスを防止するための物理的な安全性の確保
- ネットワーク要素、保存された情報、サービス、およびアプリへのアクセスを認証された人のみに許可するためのアクセス制御手段（ロールベースなど）。
- セキュリティパッチのタイムリーな更新を保証する一般的なパッチ管理の実施
- 不正なコード実行を防止するためのマルウェア対策
- 安全性の意識向上の研修

## 3.6 SaMD（医療デバイスとしてのソフトウェア）オーソ スライス 3Dニーナビゲーションソフトウェア

オーソスライス3Dニープランニングソフトウェアは、WindowsベースのPCで動作する。

| 仕様 | 商品説明 |
|---|---|
| **オペレーティング・システム** | Windows 10版 |
| **CPU** | Intel Core i7-4770以上 |
| **RAM** | 32GB以上 |
| **ディスク容量** | プログラムインストール用12GB、患者データ保存用500GB以上 |
| **モニター解像度** | 1920*1080ピクセル以上 |
| **グラフィック** | 4GB以上の専用メモリ（例:Nvidia Quadro RTX3000やNVIDIAT600など） |
| **通信ポート** | USB2.0以上 |
| **任意マウス（左ボタン、右ボタン、スクロール機能付き）** | |

**備考:**

- 患者データをローカルネットワーク・ドライブから読み込む場合、システムを起動する前にネットワークに接続されていることを確認する。ネットワーク接続に障害が発生した場合、データの読み込みに通常より時間がかかることがある。症例の読み込み中にネットワークに障害が発生した場合、ソフトウェアがユーザーに通知する。
- 他のデバイスとの互換性についての情報である。CTデータを転送する外付けハードディスクは、USB2.0以上の規格に対応している必要がある。
- その他のセキュリティに関する要件については、本マニュアルを参照する。

# 04 PII と PHI の管理

オーソスライス3Dニープランニングソフトウェアは、外科医のノートパソコン以外の場所で個人情報/PHI を処理することはない。HDO は、オーソスライス3Dニープランニングソフトウェアを含むノートパソコンを完全に管理し、そこにあるすべての PII /PHI に対して責任を負うものとする。ソフトウェアは、DICOM CT データまたは外科医が入力した PII /PHI 情報を表示するだけで、外科医のノートパソコン以外で処理することはない。HDO とユーザーは、ノートパソコン内の PHI と PII データを完全に管理し、HDO データ保持ポリシーに基づいて削除するデータがある場合、HDO/ユーザーは保持する必要のないデータを削除するために Stryker からサポートを受けることができる。

## 4.1 患者のPHIへのアクセス要求の処理

上記の「PIIとPHIの管理」の項を参照する。ユーザー/HDOは、ノートパソコンに保管されている患者データを完全に管理することができる。アプリケーションには患者の要求に応じてアクセスするための追加機能はない。HDOはHDOのプロセスに従って、患者から個人ヘルス情報開示請求があった場合は報告の出力をおこない、患者と共有する必要がある。

## 4.2 PIIの保管と削除

Stryker は外科医のノートパソコン以外では処理しない。HDO は、オーソスライス3Dニープランニングソフトウェアを含むノートパソコンを完全に制御し、すべての個人情報の保護に関する責任を負う。

PIIは、外科医からソフトウェアに提供される入力DICOMファイルに埋め込まれている。ソフトウェアはPII データを使用してGUIに表示し、最終的なプランニングPDFにはDICOMファイルからのPII情報が含まれている。

PIIデータは、ユーザーのノートパソコン内の揮発性メモリに保持され、PDFファイルに書き出すことができる。PIIデータは、他のシステムには転送されない。ユーザーはトレーニングやHDOのプライバシー要件をサポートするために、外部の利害関係者にデータを提示する目的で、ソフトウェアのGUI上で患者名を匿名化することができる。

PIIデータのバックアップとリストアについては、必要に応じてStrykerのカスタマーケアに連絡してサポートを求める。

# 05 自動ログオフ機能

HDOのITポリシーに基づき、使用されない時間が経過すると自動的に画面がロックされるよう、Windows OSを設定することを勧める。

このアプリケーションは、設定可能なタイムアウトの間、不活発の後に画面をロックする機能も備えている。ユーザーは、非アクティブ時のタイムアウトを設定することができます。詳しくは、ユーザーマニュアルの「システム設定を行う」をご覧ください。

# 06 監査統制

Strykerは、強力な保護メカニズムを使用して監査ログを不正な第三者による改ざんから保護しているため、ユーザーに余分な手順を要求することはない。監査ログは情報の改ざんを防ぐため、256-bit AES暗号を使用して暗号化されている。監査ログの復号化は、当局からの要請に応じてStrykerが対応する。ユーザーは監査ログを編集したり、変更したりすることはできない。

オーソスライス3Dニープランニングソフトウェアは、以下の種類の監査イベントを取得する。

- 患者PIIデータの作成･変更履歴（PIIデータは保存されていない。）
- リムーバブルメディアからのDICOMデータ取り込み
- アプリプログラミングインターフェース(API)および印刷のために使用類似の活動やPDF表示
- タイムスタンプ情報を付与し、取得･保存時期に応じて削除対象として選択ができるマークされたデータ。患者データの保存･更新作業を行う作業ステップ。アプリデータ - 実行されたワークフローと機能

監査ログのフォーマット:<タイムスタンプ>,<ユーザー>,<コンポーネント>,<機能/モジュール>,<アクション>

USBなどの物理媒体の安全性を考慮し、物理媒体経由でログを書き出すことも可能であるが物理メディアを安全に保管し、最新の脅威に対してアップデートすることが推奨される。

以下は、USBメモリなどの物理メディアを保護するために実施できる安全対策である。

### USBドライブを他のコンピュータに接続しない

物理デバイスに対する潜在的なセキュリティ脅威となる可能性があるので、そのコンピュータシステムの身元と安全性を確認せずに、USBをコンピュータに接続しないでください。

### セキュリティ機能の利用

USBメモリにはパスワードや暗号化機能を使い、データを保護し、またドライブを紛失した場合に備えて、情報のバックアップを取る。

### 自動実行の無効

Autorun機能は、CD、DVD、USBドライブなどのリムーバブルメディアをドライブに挿入したときに、自動的に開くようにする機能である。オートランを無効にするのは感染したUSBメモリ内の悪質なコードが自動的に開くのを防ぐ。

### セキュリティソフトウェアの使用と維持、およびすべてのソフトウェアの最新の状態の維持

コンピュータを攻撃されにくい状態にし、ウイルス定義を最新の状態に保つために、ファイアウォール、アンチウイルスソフト、アンチスパイウェアソフトを使用する。また、必要なパッチを適用して、コンピュータのソフトウェアを常に最新の状態に保つ。

## 07 認可

オーソスライス3Dニープランニングソフトウェアを完全に機能させ、作動させるためにStrykerからのみ取得できる有効なライセンスが必要である。有効なライセンスを必要とする以外に、アプリケーションのユーザーは、ソフトウェアやデータへのユーザーアクセスのために、ウィンドウズの認証·認可メカニズムを活用する必要がある。そこで、Strykerは以下に述べる通りノートパソコンに適切なユーザー認証を設定することを勧める。

システム安全性における認可とは、特定のリソースや機能にアクセスする許可をユーザーに与えることである。安全な環境では、認証の後に必ず認可が必要である。ユーザーは、組織の管理者が要求されたリソースへのアクセスを許可する前に、まず自分の身元が本物であることを証明する必要がある。そのため、セキュリティを強化するために、システムレベルで適切な認可を実装する必要がある。認可に対するさまざまなアプローチには、次のようなものがある。

### ロールベースアクセス制御（RBAC）

ユーザーは、どのような権限を持つか規定されたロールに属していることが確認される。さらに、ユーザーIDによって、アクセスできるデータも制限される。

### アクセス制御リスト(ACL)

ACLは、どのユーザーが特定のリソースにアクセスできるかを指定する。例えば、あるユーザーが特定のファイルやフォルダにアクセスしたい場合、特定のデータにアクセスできるようにするために、ユーザー名や詳細情報をACLに記載する必要がある。

## 7.1 アクセスの防止

オーソスライス3Dニープランニングソフトウェアでは、組み込まれたアクセス防止機能を有効にしておらず、Windows·アクセス防止機構を利用している。カスタマーには、以下のような適切なアクセス制御を行うことを勧める。

システムおよびソフトウェア·コンポーネントへの不正アクセスを防止するための対策を講じることは、他者によるスパイウェアのインストールや重要なファイルの削除、あるいはウイルスの作成を防ぐなど、さまざまな理由から重要である。不正アクセスを防ぐためにコンピュータに変更を加えることは、個人のプライバシーを保護することにもなる。ここでは、コンピュータを適切に保護し、他人がアプリデータにアクセスしたり変更したりするのを防ぐための手順である。

- ユーザー認証のためのパスワード保護の設定:不正なユーザーがシステムにアクセスできないように、システムレベルでパスワード保護を有効にする必要がある。パスワードは、簡単に推測できないように設定しなければならない。また、システムの全体的な安全性を強化するために、強力なパスワードポリシーを実装する必要がある。

- ウイルス対策ソフトやスパイウェア対策ソフトの導入:優れたアンチウイルスまたはスパイウェア保護プログラムがシステムに設定される必要がある。これらのプログラムは、システムやインストールされたアプリケーションの脅威として使用される可能性のある悪意のあるアクションやプログラムを検出するために使用される。最後に、これらのウイルス対策プログラムは、最新の安全脅威からシステムとインストールされたアプリを保護することができるように、定期的に更新する必要がある。

- システムへのアクセスを、信頼できる限られた人たちだけに制限することができる。これにより、インストールされたアプリは、許可された個人のみがアクセスできるようになる

## 7.2 特権とアクセス

Stryker では、ノートパソコン管理者が、同じノートパソコンでオーソスライス3Dニープランニングソフトウェアにアクセスするために、適切な権限を持つ別のユーザーを作成することを推奨している。オーソスライス3Dニープランニングソフトウェアの特権とアクセスは、

アプリのいかなるユーザーも、その意図された用途内でのみ使用でき、アプリの範囲外の他の機能は可能な限り制限されなければならないものとする。ユーザーは、異なるログインアクセスを設定することで、他のユーザーのデータにアクセスすることなく、同じノートパソコンで自分のデータを管理することができる。

# 08 サイバーセキュリティ製品更新

このアプリケーションには、更新プログラムのインストール·ポリシーが実装されていない。したがって、ユーザーはオンラインアップデートを取得することはできない。Stryker が潜在的な脆弱性を発見し、カスタマーのサイトでのアップデートが必要となった場合、ソフトウェアの新バージョンがリリースされ、カスタマー側で取るべき措置が通知される。

オペレーティング·システム、第三者の·コンポーネント（ある場合）、ウイルス対策ソフト/マルウェア対策ソフト、ファイアウォールなどの他のアプリの最新パッチを更新するのがHDOの責任である。それとも、システムの安全性·保護性を確保するためのタイムリーな対応である。

オーソスライス3Dニープランニングソフトウェアには、マルウェア対策は組み込まれていない。したがって、ユーザーは、ノートパソコンにマルウェア対策のソフトウェアを設定することを勧める。

# 09 ヘルスデータの非同定化

オーソスライス3Dニープランニングソフトウェアは、実行時にデータを匿名化するが、削除や除去は行いない。これは、アプリ自体のGUIインターフェースから行うことができる。

詳しくは、取扱説明書「追加ツール」をご覧ください。

# 10 データのバックアップと障害回復

このアプリケーションには、データのバックアップやリカバリーのためのオンラインまたはオフラインのモードは含まれていないので、ユーザーは、データのバックアップを物理的なメディアやオンラインストレージを介して、自分自身のコピーを持つことが期待される。

# 11 ヘルスデータの整合性と真正性

システム上に保存されたヘルスデータやその他の機密データは、データの完全性を保持するために、アプリ自身が強力な256-bit AES暗号化アルゴリズムを用いて暗号化するため、ユーザーの操作は必要ない。アプリは、データを読み込む前に、その整合性を適切にチェックする。

# 12 マルウェア検知・防御

オーソスライス3Dニープランニングソフトウェアには、初期状態でマルウェア検出機能が含まれていないため、ユーザーが何らかのマルウェア検出機能を導入している必要がある。マルウェアの検出は、マルウェアやサイバー攻撃に関するコンピュータの早期警告システムとして機能するため、マルウェアの事前対策として非常に重要である。ハッカーをコンピュータから排除し、情報の漏洩を防ぐことができる。これには、コンピュータとファイルをスキャンしてマルウェアを検出するプロセスが含まれる。

マルウェア対策として、以下の点を推奨する。

- システムに優れたマルウェア検出プログラムをインストールする
- コンピュータとソフトウェアを常に最新の状態に保つ
- できるだけ管理者以外のアカウントを使用する
- リンクのクリック、何かをダウンロードする前にはよく考えてください。
- メールの添付ファイルや画像の開封に注意する
- ソフトウェアのダウンロードを要求するポップアップ・ウィンドウは信用しないこと
- ファイル共有を制限する

## 12.1 その他の補償/保護コントロール

オーソスライス3Dニープランニングソフトウェアは、アプリケーションを正しく動作させるために有効なライセンスを必要とし、ログは秘密鍵を用いて暗号化され、実行時にデータを匿名化するなど、その設計上いくつかの保護機構を備えている。また、以下のような安全対策を実施することを推奨する。

- アプリケーションは、Windows OSの組み込まれているメカニズムを使用して、許可された個人のみ実行できる必要がある。
- オーソスライス3Dニープランニングが悪意あるものとして認識されないように、デバイス上で動作するすべての保安要員で適切なアプリホワイトリストを作成する必要がある。
- システムにインストールされている第三者製のコンポーネントは、適切に更新する必要がある。

- 可能性のある脅威を排除するため、定期的にアンチウイルスの検査を実施すること。
- アプリケーションのログを監査し、エラーや正常な動作を確認する。
- 定期的なWindowsアップデートとパッチをインストールしておく必要がある。

## 12.2 ファイアウォールの実装

このアプリケーションを安全に使用するために、以下のファイアウォール規則を厳守する必要がある。

ファイアウォールが有効になっていることを確認してください。有効になっていない場合は、Windowsパソコンで以下の手順を実行してください。

1. スタートメニューから「コントロールパネル」をクリックする。
2. 「システムとセキュリティ」を選択します。「Windows Defender ファイアウォール」をクリックする。
3. 「Windows ファイアウォールをオンまたはオフにする」をクリックする。
4. ドメインホーム/ワーク（プライベート）またはパブリックネットワークで「Windowsファイアウォールをオンにする」を選択する。

### その他、考慮すべき事項

- ログや警告がユーザーの注意を引くことは必須である。異常があれば、それに対処した後に解決しなければならない。
- アプリケーションの機能に必要なポートには、許可されたクライアントのみがアクセスできることを確認する。
- システム上にマルウェアが報告された場合、通常業務を再開する前に、適切な掃引スキャンが開始され、マルウェアの除去が成功したことを確認する。

ファイアウォールは、デバイスへのネットワークアクセスを防止するのに役立つ。適切に使用・設定されれば、保護された信頼性の高いアクセスを実現することができます。外部からの脅威、IPスプーフィングやルーティング攻撃、悪意のあるパケットに対する不正アクセスやネットワーク接続を防止するのに役立つ。

# 13 コネクティビティ能力

既定のオーソスライス3Dニープランニングソフトウェアは、ネットワーク接続やワイヤレス接続を必要としない。入力されたCTデータはネットワークドライブから読み込むことができ、HDO ITはオーソスライス3Dニープランニングソフトウェアがインストールされているノートパソコンに接続されたネットワーク・ドライブを保護するために十分なセキュリティコントロールを確保する。また、データバックアップやデータ転送のために物理メディアをシステムに挿入する必要がある場合の制限も適用されない。

そのため、必要な場合は、安全で最新の物理メディアのみを使用したほうがよい。USBや物理メディアを保護するために、優れたウイルス対策プログラムを使用して適切にスキャンすることが最善である。

# 14 個人認証

オーソスライス3Dニープランニングソフトウェアは、システム独自の運用が可能となる有効なライセンスが必要なこと以外にいかなる認証メカニズムも提供されていない。

Strykerは、ノートパソコンに強力なパスワードベースの認証を使用した安全なWindows認証を導入することを推奨する。これらのパスワードは、簡単に推測できないような強力なものである必要がある。また、パスワードには英数字と特殊文字が含まれている必要があり、最高のセキュリティを確保することができる。

適切なユーザー管理を行うためには、以下の点を考慮したシステム構成が必要。

- 認証システムは、パスワードベースのログインまたは統合されたWindowsベースの認証によって行われる必要があること。
- 数回失敗すると、アカウントがロックアウトされること。
- パスワードは一定期間ごとに変更すること。
- デフォルトのパスワードや推測しやすいパスワードは、システムで受け入れてはならない。パスワードはパスワードの複雑さのポリシーを満たしている必要があること。
- 適当な時間が経過して使用していない状態になると、ロックされるように設定されている必要があること。
- システムへのアクセスを管理するために、物理的なセキュリティを実装する必要があること。

## 15 デバイスのライフサイクルにおける第三者製コンポーネントのロードマップ

Stryker は、IEC 62304 で規定されている要件に従って第三者製コンポーネントを評価し、アプリに適切な措置を講じている。

Stryker は、リスクの高い第三者製のコンポーネントを定期的に評価し、製品ライフサイクル中に必要な更新があれば、カスタマーに知らせる。

## 16 システムおよびアプリの堅牢化

Strykerはオーソスライス3Dニープランニングソフトウェアのアプリセキュリティテストとセキュリティコードレビューを実施した。オーソスライス3Dニープランニングソフトウェアは、セキュリティ問題につながる脆弱性や欠陥を排除し、ハード化されている。

システムの堅牢化とは、アプリケーション、システム、その他の領域における脆弱性を低減するためのツール、テクニック、最善の措置の集合体である。システムの堅牢化の目的は、潜在的な攻撃ベクトルを排除し、システムの攻撃対象領域を凝縮することによって、セキュリティのリスクを低減することである。不要なプログラム、アカウント機能、アプリケーション、ポート、認可、アクセスなどを取り除くことで、攻撃者やマルウェアがITエコシステムの中で足場を固める機会を減らすことができる。システムの堅牢化には、潜在的なセキュリティ脆弱性を監査し、特定し、閉鎖し、制御するための体系的なアプローチが必要である。実施するハードニングの種類は、既存技術のリスク、利用可能なリソース、修正を行う優先順位によって異なる。

Strykerは、システムの堅牢化を実施する際に、以下の点に留意することをカスタマーに推奨している。

### 既存のシステムの監査

既存技術の包括的な監査を実施する。侵入テスト、脆弱性スキャン、構成管理、その他のセキュリティ監査ツールを使用して、アプリケーションがインストールされているシステムの欠陥を発見し、修正に優先順位をつける。

### システム堅牢化の戦略策定

すべてのシステムを一度にハード化する必要はない。むしろ、テクノロジー・エコシステム内で特定されたリスクに基づいて戦略と計画を立て、段階的なアプローチで最大の欠陥を是正する。

### 脆弱性を直ちに修正する

自動的かつ包括的な脆弱性特定とパッチ適用システムを確実に導入する。

### ネットワークのハード化

ファイアウォールが適切に設定され、すべてのルールが定期的に監査されていること;リモートアクセスポイントやユーザーの安全確保;未使用または不要なオープンポートのブロック;不要なプロトコルやサービスの無効化および削除;アクセスリストの実装;ネットワークトラフィックの暗号化である。

13項もご参照ください

### オペレーティングシステムのハード化

OSのアップデート・サービスパック・パッチの自動適用;不要なドライバー・ファイル共有・ライブラリ・ソフトウェア・サービス・機能の削除;ローカルストレージの暗号化;レジストリやその他のシステム権限の強化;すべての活動・エラー・警告の記録;特権ユーザーの制御の実装であること。

### 不要なアカウントや権限の排除

ITインフラ全体を通じて不要なアカウント（著作権者不明アカウントや未使用アカウントなど）や特権を削除し、最小限の特権を強制すること。

### マルウェア対策のインストール

オーソスライス3Dニープランニングソフトウェアが動作するシステムには、適切なマルウェア対策ソフトウェアが最新のアップデートでインストールされている必要がある。

## 17 ヘルスデータ保管の機密性

保存データは、機密性の高い医療データを覗き見から保護するアプリケーションに実装された強力な暗号化メカニズムによって暗号化される。

## 18 送信の機密性

オーソスライス3Dニープランニングソフトウェアは、ネットワークやインターネットにデータを送信しない。エンドユーザーは、取り外し可能なメディアやローカルシステムを使用して、ソフトウェアにデータを入力する。出力したpdfは、取り外し可能なメディアに保存したり、書き出したりすることができる。

以下は、データの機密性を管理する際に遵守すべき、ユーザーへのガイドラインである。

### データアクセスの管理

機密保持の管理は、誰がデータにアクセスできるかを管理することに大きく関わってきます。アクセスは、「知る必要がある」人にの

### 物理的に安全なデバイス

み自動化され、許可されるようにすることが、不必要な露出を抑える上で大きな意味を持つ。また、ユーザーは強力なパスワードと、実用的であれば二要素認証でアクセスを認証する必要がある。定期的にアクセスリストを見直し、不要になったアクセスは速やかに取り消す。

データへのアクセスを制御することは、デジタルと物理の両面であらゆる種類のアクセスを制御することを意味する。デバイスを鍵のかかる場所に保管し、誤用や盗難から保護する。デバイスや機密文書を公共の場に放置しない。

### データの安全な廃棄

利用目的の達成に必要でなくなったデータは、適切に廃棄しなければならない。

### データ取得の管理

機密データを収集する際には、実際にどの程度のデータが必要なのかを意識し、プライバシーや機密保持について慎重に検討した上で、取得するようにする。必要な場合を除き、機密データの取得を避ける。機密保持のリスクを減らす最善の方法の一つは、そもそも収集する機密データの量を減らすことである。

### データ活用の管理

機密データを承認された必要な範囲でのみ使用することにより、機密保持のリスクをさらに低減することができる。機密データを誤って使用すると、そのデータおよびそのデータが表す個人またはグループのプライバシーと機密性が侵害される。

### ノートパソコンの管理

コンピュータの管理は、多くの重要なセキュリティ対策が含まれる幅広いテーマである。デバイスを保護することで、デバイスに含まれるデータも保護することができる。ウィルス対策ソフトウェアの使用、定期的なソフトウェアのパッチ適用、アプリケーションのホワイトリスト化、デバイスのパスコードの使用、非アクティブの Web セッションの一時停止、ファイアウォールの有効化、ディスク全体の暗号化など、サイバーセキュリティの基本的な衛生管理に従う。

## 19 セキュリティ・プログラムの統合

オーソスライス3Dニープランニングソフトウェアは、ユーザーのラップトップにインストールされるスタンドアローンのソフトウェアである。このソフトウェアの安全な使用方法は、このドキュメントのセクション 8 で説明されている。

Strykerは、本製品に関する苦情処理プロセスの一環として、事故対応プログラムを実施している。本製品は日本市場のみを対象としており、ユーザーは T/F: 本ソフトウェアに潜在的な脅威が発見された場合は、03-6894-0000 にご連絡ください。本製品は日本国内向けであり、万が一、本ソフトウェアに潜在的な脅威が確認された場合は、お電話（03-6894-0000）にてご連絡ください。
Strykerは、オーソスライス3Dニープランニングソフトウェア・アプリケーションのセキュリティテストを徹底的に行い、外部からの脅威から確実に保護するための適切な対策を実施している。しかし、このようなセキュリティ対策を実施するだけでなく、ユーザーにはより良いセキュリティ体制を確保するために、以下のガイドラインに従って一歩先を行くことを勧める。

- USBなどの未知の物理メディアを接続しないでください。デバイスに接続する必要がある場合は、強力なマルウェア対策プログラムを使用して徹底的にスキャンする必要がある。
- - マルウェア対策ソフトやアンチウィルスソフトを使用して、潜在的な脅威がないか定期的にスキャンすること。

### 19.1 リスクマネジメント

Stryker は、サイバーセキュリティ・リスク管理を、健康と安全のリスク管理のための全体的なプログラムに統合している。EN/ISO 14971 とストライカー製品セキュリティ手順に準拠したガイドラインに従って、本デバイスのセキュリティと安全性の両方のリスク評価が実施された。さらに、ストライカーは、本デバイスの継続的なセキュリティ姿勢を監視し、発生しうるセキュリティインシデントに対処する、堅牢な市販後セキュリティリスク管理プロセスを有している。

## 20 13 安全な廃棄物処理

安全な廃棄のために、Stryker Customer Careにご連絡ください。

**Distributed by:**
**Stryker Japan K.K.**
2-6-1, Koraku, Bunkyo-ku,Tokyo, 112-004, Japan
t/f: 03-6894-0000

700001920536 / AE

**Stryker Global Technology Center Private Limited**
Vatika Business Park, 10th Floor
Block 2, Sector-49
Sohna Road
Gurgaon 122002
Haryana
India
www.stryker.com